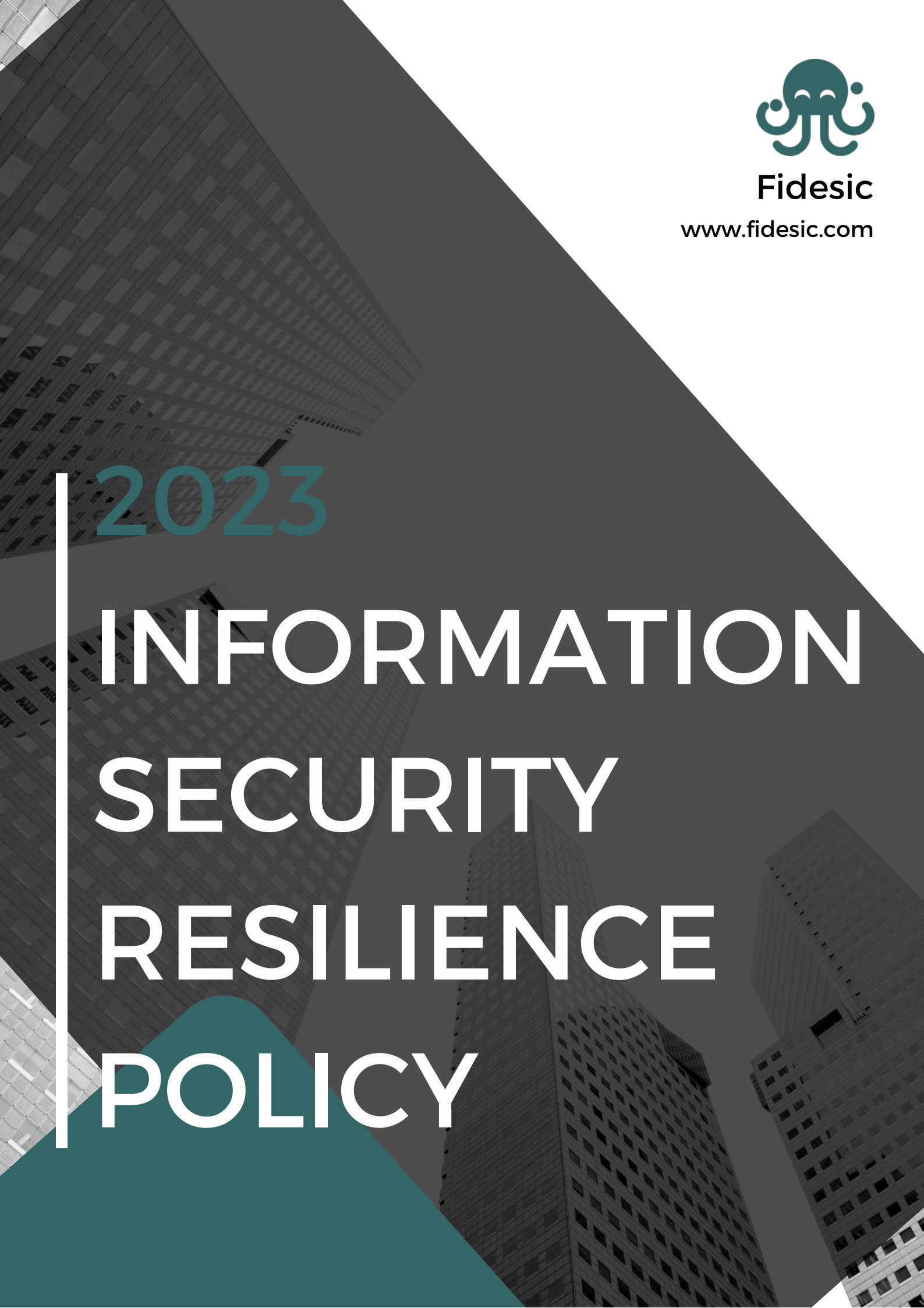

Fidesic

www.fidesic.com

2023

INFORMATION SECURITY RESILIENCE POLICY

Introduction

The Information Security Resilience Policy (ISRP) objective is to establish a business resiliency framework to help provide continuity in response to business interruption events affecting Fidesic's regular operations.

The ISRP approach is built upon several programs: emergency response, crisis management of incidents, technology emergency recovery and business continuity. The objective of this program is to minimize negative impacts to Fidesic customers and maintain critical business processes until regular operating conditions are restored.

The Fidesic ISRP is designed to engage several aspects of emergency management and business continuity from the onset of an event and adapt based on the needs of the situation.

Responsibilities

The ISRP goal is to establish a framework for resilience that helps provide a streamlined response to business interruption events affecting Fidesic. Business continuity is the key program within this framework.

Business continuity policies, practices, and standards are aligned with International Standards Organization (ISO) Business Continuity Management Systems guidance.

The Fidesic Security Board is responsible for providing guidance to the internal team , to help them complete their roles and responsibilities defined in this policy. As a part of this guidance, the Security Board develops planning materials and tools meeting the policy requirements for managing their business continuity plans, testing and training procedures.

The Security Board are involved within the functional business continuity planning. FSB members are required to conduct an annual review of their business continuity plan with their objective of maintaining operational recovery capability, dependent upon changes to the risk environment as well as new business processes.

Fidesic Security Board Planning Responsibility

- Identify possible business interruption scenarios, including peoples, resources and facilities
- Conduct a Business Impact Analysis that specifies a recovery timeline, and recovery competency goal
- Define a business continuity plan and procedure to effectively manage and respond to various risk scenarios.
- Provide feedback on revisions to business continuity plans based on changes to operations or relative risk
- Educate personnel on contingency planning procedures
- Implement their business continuity plans as needed

Continuity

The Fidesic ISRP objective is to establish a business resiliency framework that helps provide a rapid response to business interrupting events. Business continuity is a key part of this program.

Business continuity policies, practices, and standards are aligned with International Standards Organization (ISO) Business Continuity Management Systems guidance.

Functional business continuity planning is managed by the FSB. The critical portions of Fidesic are required to annual review of the business continuity plan with the objective of maintaining operation recovery capability, reflecting changes to the business or risk environment.

All critical business functions require

- Review and update of a Risk Assessment
- A written business impact analysis that includes identification of interdependent resources and a determination of a recovery timeline, and recovery competency goal
- A Defined business continuity strategy
- Annual review and update to a Business Continuity Plan
- Have regular training with employees on Business Continuity Planning
- Conduct exercises to test the efficacy of the plan within each critical business function.
- Implement lessons learned for plan improvement
- Obtain attestation from The Fidesic Security Board

Following their review, The Fidesic Security Board records all details on the appropriate security board scorecard.

Resilience and Disaster Recovery

The Fidesic ISRP objective is to establish a business resiliency framework that helps provide a rapid response to business interrupting events. Disaster recovery is a key part of this program.

Fidesic's Disaster Recovery plan focuses on the resilience of computing infrastructure supporting Fidesic's internal operations and product. Fidesic's production data centers are hosted on Azure, and separated into different regions based on Azure's best practices. All environment

Fidesic has identified certain systems that can be backed up and restored

- Database: full and incremental backups are created on physical and electronic media
- Archive Logs: full and incremental backups are created on physical and electronic media
- Source code repository backups are performed on a recurring basis.

Additional strategies for critical internal systems

- Azure Site Recovery Failover
- Current copy of production databases stored at a second region
- Redundant middle or application server tiers made up of a set of servers to distribute application functionality across multiple host machines

Fidesic maintains a redundant network infrastructure, including NDS servers to route between primary and secondary sites, network devices and load balancers.